UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the following Facebook User ID:: https://www.facebook.com/josh.rackedup, Facebook ID # 100015783785535

Case No. 21 MJ 90

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Wis. Stat. § 940.01(1)(a), Wis. Stat. § 939.05 and Title 18, USC, Section 1073	See attached affidavit

The application is based on these facts:

See attached affidavit

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Bryon Downey
Digitally signed by Bryon Downey
Date: 2021.04.13 10:57:35 -05'00'

Applicant's signature

USMS, TFO Bryon Downey

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone/email *(specify reliable electronic means)*.

Date: April 13, 2021

William E. Duffin

Judge's signature

City and state: Milwaukee, WI.

Honorable William E. Duffin

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APLICATION FOR A SEARCH WARRANT

I, Bryon Downey, being duly sworn, hereby depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Police Officer with Milwaukee Police Department for approximately 18 years and assigned to the U.S. Marshals Fugitive Task Force and, as such, am charged with enforcing all laws in all jurisdictions of the United States, its territories, and possessions. I have investigated multiple fugitive cases including State, Federal subjects. I have had previous experiences using the social media site of Facebook in order to locate and apprehend Fugitives from Justice. I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. Section 2510(7), in that I am empowered by law to conduct investigations.

2. This Affidavit is made in support of an application for a search warrant to search the Target Account, more fully described in Attachment A, for evidence, instrumentalities, and proceeds, more fully described in Attachment B, 1st Degree Intentional Homicide contrary to Wis. Stat. § 940.01(1)(a) with a modifier of PTAC, as a Party to a Crime in violation of Wis. Stat. § 939.05. An arrest warrant (Milwaukee Police Department warrant number K01454) and authorization for nationwide extradition were issued the same day for Santos M SOLIER, (M/W 12/21/97 and Unlawful Flight to Avoid Prosecution in violation of Title 18, United States Code, Section 1073.

3. The facts set forth in this Affidavit are based upon my personal observations, my training and experience, and information obtained from other law enforcement agents and witnesses. This Affidavit is intended to show that there is probable cause to believe that evidence, instrumentalities, and proceeds, more fully described in Attachment B, for the subject

offenses listed above will be found in the subject accounts, more fully described in Attachment A, and does not purport to set forth all of my knowledge of or investigation into this matter.

STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

4. Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

a. Title 18, United States Code, Section 2703(a) provides, in part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Title 18, United States Code, Section 2703(b) provides, in part:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection
>
> > (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant□.
>
> (2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service
>
> > (A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computer service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. The government may also obtain records and other information pertaining to a subscriber to or customer of electronic communication service or remote computing service by way of a search warrant. See 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. See 18 U.S.C. § 2703(c)(3).

d. The statute permits the warrant to be served on the provider, who will then disclose the relevant records to the officer, who need not be onsite at the time the search is executed. Title 18, United States Code, Section 2703(g), provides, in part:

Presence of Officer Not Required Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

e. Title 18, United States Code, Section 2711, provides, in part:

As used in this chapter

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

f. Title 18, United States Code, Section 2510, provides, in part:

(8) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .

(14) "electronic communications system" means any wire, radio, electromagnetic, photo optical or photo electronic facilities for the transmission of wire or electronic communications, and any computer

> facilities or related electronic equipment for the electronic storage of such communications; . . .
>
> (15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications; . . .
>
> (17) "electronic storage" means
>
> > (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
> >
> > (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

FACEBOOK TECHNICAL BACKGROUND

5. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts through which users can share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

6. Facebook asks users to provide basic contact information, either during the registration process or thereafter. This information may include the user's full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

7. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information in the user's account available only to himself or herself, to other specified Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account

settings that users can adjust to control, for example, the types of notifications they receive from Facebook. Depending on the user's privacy settings, Facebook may also obtain and store the physical location of the user's device(s) as they interact with the Facebook service on those device(s).

8. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

9. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

10. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she

receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

11. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

12. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

13. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.

14. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.

15. Some Facebook pages are affiliated with groups of users, rather than one individual user. Membership in the group is monitored and regulated by the administrator or

head of the group, who can invite new members and reject or accept requests by users to enter. Facebook can identify all users who are currently registered to a particular group and can identify the administrator and creator of the group. Facebook also assigns a group identification number to each group. Facebook uses the term "Group Contact Info" to describe the contact information for the group's creator and administrator, as well as the current status of the group profile page.

16. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

17. Facebook also retains IP address logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action.

18. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service used, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical

problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

19. Therefore, the computers of Facebook are likely to contain all the material just described, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and account application.

PROBABLE CAUSE

20. On March 30, 2021, a criminal complaint was issued in Milwaukee County Circuit Court, case number 2021CF001209, charging SOLIER with one count of 1st Degree Intentional Homicide contrary to Wis. Stat. § 940.01(1)(a) with a modifier of PTAC, as a Party to a Crime in violation of Wis. Stat. § 939.05. An arrest warrant (Milwaukee Police Department warrant number K01454) and authorization for nationwide extradition were issued the same day.

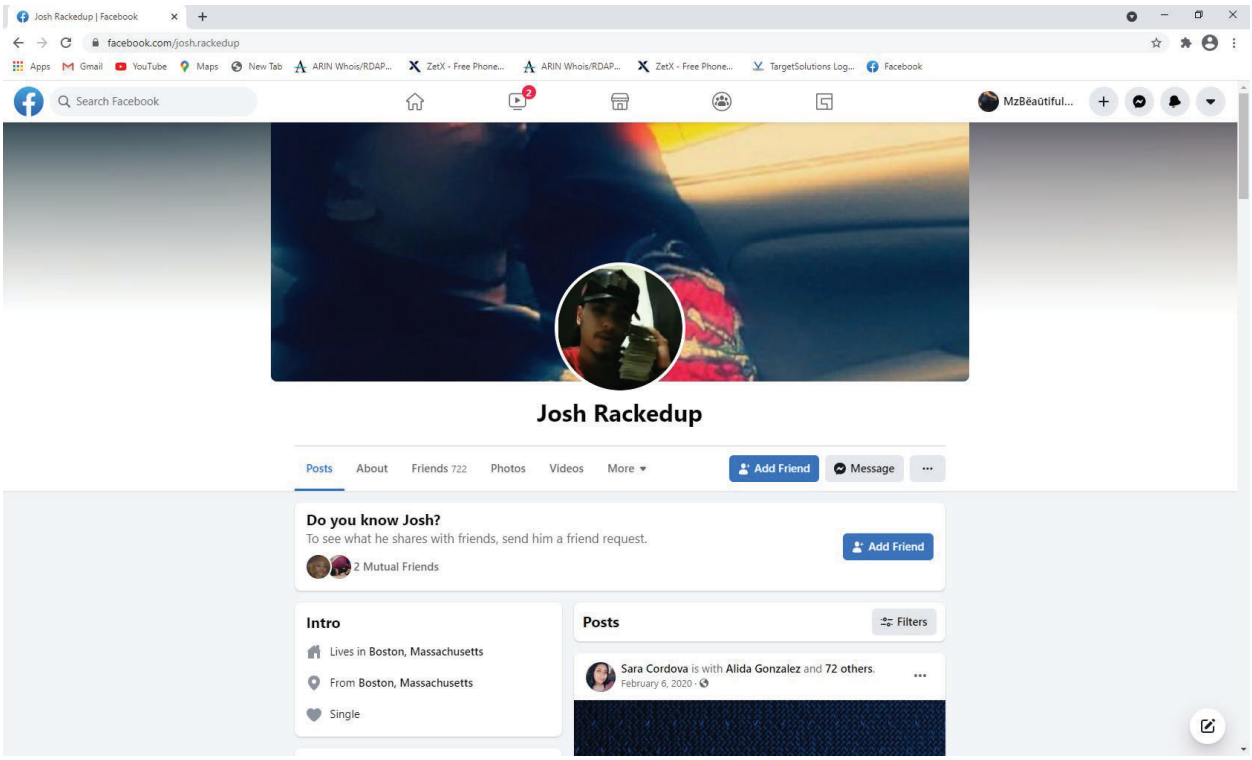
21. Since the issuance of the arrest warrant, the Milwaukee Police Department Fugitive Apprehension Unit & USMS has made multiple attempts at apprehending SOLIER, but SOLIER was able to flee the state in attempt to avoid prosecution.

22. On Monday, March 30th, 2021 Lt. Patrick Pajot of the Milwaukee Police Department's Homicide Unit, received information from a Confidential Informant, (Hereinafter CI), that SOLIER and Byrell C Bonds, (m/b 8/26/96), who is co-actor in this offence, were running to Florida.

23. On April 6, 2021, Sgt. Santos, Chicago Police Department assigned to The Great Lakes Regional Fugitive Task Force-Chicago went to Chicago O'Hare international Airport and received confirmation that both Bryell C. BONDS & Santos M. SOLIER, flew out of O'Hare using Spirit Airlines on March 29th to Dallas/Fort Worth International Airport and then to Fort Lauderdale-Hollywood International Airport FL.

24. On 4/8/21, An Unlawful Flight to Avoid Prosecution in violation of Title 18, United States Code, Section 1073 arrest warrant was issued for SOLIER, in relation to those charges, he remains a fugitive from justice. The United States Marshals Service is leading the investigation in order to locate and arrest SOLIER.

25. On 4/7/21, Det. Thaddeus SCHIMMELS of Milwaukee Police Homicide Unit, received a call/tip from confidential source, (Hereinafter CS), this Source has provided information to both Det. SCHIMMELS and myself to be trueful and accurate regarding SOLIER and family. CS provided SOLIER's Facebook account that he is currently using, Facebook URL, https://www.facebook.com/josh.rackedup, Facebook ID # "100015783785535".



26. On April 7th your affiant looked up Facebook account for fugitive Santos SOLIER, using an open source search of Facebook.com The account located under url: https://www.facebook.com/josh.rackedup, Facebook ID # "100015783785535", has a screen name of "Josh Rackedup".

27. Your affiant was able to identify the account as being SOLIER, by comparing DOT and Booking photos to the photos depicted in the publicly displayed photos within the account.

28. The affiant believes that information from this Facebook account will assist the United States Marshals Fugitive Task Force in locating and arresting fugitive from justice Santos SOLIER.

CONCLUSION

29. Based on the facts set forth in this Affidavit, your Affiant submits that there is probable cause to believe that the subject accounts contain the fruits, instrumentalities, and evidence of the subject offenses.

ATTACHMENT A

This Search Warrant is being sought for the data specified in Attachment B associated with the following Facebook User ID: https://www.facebook.com/josh.rackedup, Facebook ID # 100015783785535

That are stored at premises owned, maintained, controlled, or operated by Facebook, a social networking company headquartered in Menlo Park, California.

ATTACHMENT B

I. Information to be disclosed by Facebook, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of Facebook, Facebook is required to disclose the following information to the government for each User ID listed in Attachment A:

(a) All physical location data collected by Facebook for the user of the account, including any data collected by Facebook's location services via the user's mobile phone or other device, on a real-time or near-real time basis. Facebook is required to provide any such data they collect, regardless of the time of day.

II. Information to be seized by the government

(a) All data disclosed by Facebook pursuant to this attachment. This data shall be made accessible by the provider to the United States Marshals Service 24/7, day or night, and/or emailed to Task Force Officer Bryon Downey with United Stated Marshals Fugitive Task force at bdowney@northcentralhidta.org.

III. Time for production by provider

The provider shall begin producing the information required by this attachment within seven (7) days of the date of service of the warrant.

IV. Duration of production

The provider shall produce the information required by this attachment for a period of thirty (30) days from the date of issuance of this warrant.